

REMARKS

In response to the above-identified Office Action, Applicants amend the application and seeks reconsideration thereof. In this response, Applicants amend claims 1, 11, and 18. Applicants do not cancel any claims or add any new claims. Accordingly, claims 1-26 are pending.

I. Claims Rejected Under 35 U.S.C. § 103(a)

Claims 1-9, 11-14, 16, 18-21, 23-24, and 26 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,748,539 issued to Lotspiech (hereinafter "Lotspiech") in view of U.S. Pre-Grant Patent Application No. 2001/0032088 applied for by Utsumi et al. (hereinafter "Utsumi"). Applicants respectfully disagree for the following reasons.

To establish a *prima facie* case of obviousness, the Examiner must show the cited references, combined, teach or suggest each of the elements of a claim. In regard to claims 1, 11, and 18, these claims include the element or method of data encryption based on "a nonce received over a data bus from a number generator." Claim 1 recites an encryption subsystem that receives the nonce over the data bus to derive the bus key, uses the bus key to encrypt the data, and subsequently sends the encrypted data over the data bus. Claims 11 and 18 recite a similar method or apparatus as in claim 1. Neither Lotspiech nor Utsumi suggests or teaches receiving the nonce over the data bus and sending the encrypted data over the same data bus.

Specifically, the Examiner characterizes Lotspiech's media ID (col. 3, lines 14-15) as the nonce. With this characterization, the nonce taught by Lotspiech is sent internally to an encryption module to generate an encryption key. The encrypted data is then stored in a flash memory and transferred to a player-record device (Fig. 1). Lotspiech not only fails to disclose transmitting the nonce over a data bus to the encryption module, but also fails to disclose using the same data bus for the encryption module to receive the nonce and to send the encrypted data. Relying on Lotspiech's teaching, one of ordinary skill in the art would place the number generator and the encryption module in the same device, which is in stark contrast to the claimed encryption subsystem where the encryption and number generator are on the opposite ends of the data bus.

The Examiner relies on Utsumi for disclosing the encryption subsystem housed within a storage device. However, like Lotspiech, Utsumi does not teach or suggest receiving the nonce over the data bus and sending the encrypted data over the same data bus. Therefore, Utsumi cannot cure the defect of Lotspiech. One of ordinary skill in the art will not be motivated by Utsumi to modify Lotspiech such that the encryption module receives the nonce over the data bus and sends the encrypted data over the same data bus.

Further, the combination of Utsumi with Lotspiech is inappropriate as this combination would alter the principle of operation of the primary reference Lotspiech. The Examiner admits in the above-identified office action that Lotspiech does not disclose an encryption subsystem housed within a storage device. Rather, the encryption module in Lotspiech is housed within a computer kiosk responsible for updating the media ID, generating an encryption key, and controlling the check-ins and check-outs of digitized music rental (see Abstract). Removing the encryption module from the kiosk to a storage device as taught by Utsumi would make it impossible for a user to rent music from the kiosk because the digitized music checked out from the kiosk would not be encrypted. Thus, the proposed combination of Utsumi with the primary reference of Lotspiech is inappropriate. See MPEP § 2143.01. Accordingly, reconsideration and withdrawal of the obviousness rejection of claims 1, 11, and 18 are requested.

In regard to claims 2-9, 12-14, 16, 19-21, 23-24, and 26, these claims depend from independent claims 1, 11, and 18 and incorporate the limitations thereof. Thus, at least for the reasons mentioned in regard to claims 1, 11, and 18, these claims are not obvious over Lotspiech in view of Utsumi. Accordingly, reconsideration and withdrawal of the obviousness rejection of claims 2-9, 12-14, 16, 19-21, 23-24, and 26 are requested.

Claims 10, 17, and 22 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Lotspiech in view of Utsumi and further in view of U.S. Patent No. 6,751,321 issued to Kato et al. (hereinafter "Kato").

Claims 10, 17, and 22 depend from independent claims 1, 11, and 18 and incorporate the limitations thereof. Thus, at least for the reasons mentioned above in regard to independent claims 1, 11, and 18, Lotspiech and Utsumi do not teach or suggest each of the elements of these claims. Further, Kato does not cure the defects of Lotspiech and Utsumi. Although Kato mentions random number generation in col. 5, lines 30-40, nothing in Kato teaches or suggests an encryption module that receives a nonce over the data bus and sends the encrypted data over the same data bus.

Claims 10, 17, and 22 are also rejected under 35 U.S.C. § 103(a) as being unpatentable over Lotspiech in view of Utsumi and further in view of the 1998 ACM article “A Practical Secure Physical Bit Generator” authored by Jakobsson et al. (hereinafter “Jakobsson”).

Claims 10, 17, and 22 depend from independent claims 1, 11, and 18 and incorporate the limitations thereof. Thus, at least for the reasons mentioned above in regard to independent claims 1, 11, and 18, Lotspiech and Utsumi do not teach or suggest each of the elements of these claims. Further, Jakobsson does not cure the defects of Lotspiech and Utsumi. Although Jakobsson mentions random number generation, nothing in Jakobsson teaches or suggests an encryption module that receives a nonce over the data bus and sends the encrypted data over the same data bus.

Claims 15 and 25 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Lotspiech in view of Utsumi and further in view of U.S. Patent Application No. 2002/0015494 applied for by Nagai, et al. (hereinafter “Nagai”).

Claims 15 and 25 depend from independent claims 11, and 18 and incorporate the limitations thereof. Thus, at least for the reasons mentioned above in regard to independent claims 11, and 18, Lotspiech and Utsumi do not teach or suggest each of the elements of these claims. Further, Nagai does not cure the defects of Lotspiech and Utsumi. Nothing in Nagai teaches or suggests an encryption module that receives a nonce over the data bus and sends the encrypted data over the same data bus.

CONCLUSION

In view of the foregoing, it is believed that all claims now pending, namely claims 1-26 patentably define the subject invention over the prior art of record, and are in condition for allowance and such action is earnestly solicited at the earliest possible date. If the Examiner believes that a telephone conference would be useful in moving the application forward to allowance, the Examiner is encouraged to contact the undersigned at (310) 207 3800.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: 3/14, 2005

Thomas M. Coester
Thomas M. Coester, Reg. No. 39,367

12400 Wilshire Blvd.
Seventh Floor
Los Angeles, California 90025
(310) 207-3800

CERTIFICATE OF MAILING:

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Mail Stop Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on March 14, 2005.

Lillian E. Rodriguez 3-14-05
Lillian E. Rodriguez March 14, 2005